(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 536 928**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **82 20052**

(51) Int Cl³ : H 04 L 9/00.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 30 novembre 1982.

(30) Priorité

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 22 du 1er juin 1984.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *ETAT FRANÇAIS, représenté par le ministre des PTT (Centre National d'Etudes des Télécommunications) et Etablissement public dit : Télédiffusion de France.* — FR.

(72) Inventeur(s) : Louis Guillou.

(73) Titulaire(s) :

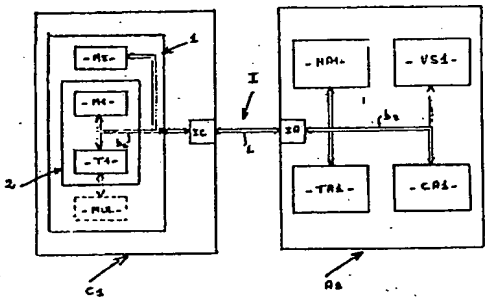
(74) Mandataire(s) : Brevatome.

(54) Système pour chiffrer et déchiffrer des informations, du type utilisant un système de déchiffrement à clé publique.

(57) L'invention a pour objet un système pour chiffrer et déchiffrer des informations, du type utilisant un système de chiffrement à clé publique.

Le système se compose d'au moins un dipositif électronique 1 avantageusement monté sur un support portatif amovible C1 tel qu'une carte, et d'un appareil A1 auquel est connecté la carte C1. Le dispositif électronique 1 comprend un microprocesseur 2 disposant d'une mémoire M1, et une mémoire morte programmable M2. Dans la mémoire M1 est enregistré un algorithme correspondant à la fonction secrète d'une fonction à clé publique du type RSEA, et dans la mémoire M2 est enregistrée la clé secrète S permettant l'exécution de cet algorithme.

L'invention s'applique notamment à la transmission de messages signés.



FR 2 536 928 - A1

Vente des fascicules à l'IMPRIMERIE NATIONALE, 27, rue de la Convention — 75732 PARIS CEDEX 15

SYSTEME POUR CHIFFRER ET DECHIFFRER DES INFORMATIONS, DU TYPE UTILISANT UN SYSTEME DE CHIFFREMENT A CLE PUBLIQUE.

L'invention concerne généralement les systèmes de transmission d'informations, notamment confidentielles, et a plus particulièrement pour objet un système pour chiffrer et déchiffrer des informations, du type utilisant un système de chiffrement à clé publique.

Avec le développement des télétransmissions, de la téléinformatique et de la télématique, il est indispensable de pouvoir s'assurer de l'origine et/ou de l'authenticité d'une information et/ou de la confidentialité de la transmission de cette information.

Ces divers aspects sont par exemple particulièrement importants dans les applications du courrier électronique, du paiement électronique et du téléphone, en particulier si l'on veut banaliser les appareils de transmission mis en oeuvre dans ces applications. Il est en effet indispensable que ces appareils mis à la disposition du public ne puissent livrer un secret de fonctionnement du système et compromettre ainsi la sécurité exigée.

Les applications précitées et plus généralement les applications personnalisées conçues pour délivrer un service, moyennant paiement, à des personnes dûment habilitées, et les applications personnalisées conçues pour échanger des informations confidentielles entre des personnes habilitées, font obligatoirement intervenir une notion de secret. Cette notion de secret a pour but d'éviter des tentatives de fraude aussi bien par des personnes habilitées que par des personnes non habilitées.

La mise en oeuvre pratique de cette notion de secret se traduit généralement par la présence d'au moins un paramètre secret, souvent dénommé clé secrète, qui intervient dans au moins une phase du processus de

déroulement d'un échange d'informations ou de délivrance d'un service. Cette clé secrète est généralement combinée avec au moins une information pour donner une information résultante publique dont le contenu et/ou l'origine ne peut être authentifié que par des personnes ou des appareils habilités. Cette combinaison est généralement effectuée par des algorithmes de calcul qui sont spécifiques des applications envisagées.

Il va être décrit ci-dessous des systèmes qui sont fondés sur des algorithmes de chiffrement susceptibles d'être utilisés pour authentifier et protéger des informations confidentielles notamment transmises entre deux personnes ou entre une personne et un appareil dispensateur d'un service.

Ces systèmes peuvent être classés en deux grandes familles :

- Une première famille de systèmes de chiffrement est fondée sur l'utilisation d'un algorithme de chiffrement réversible et public dont le plus connu est le DES. Ce système nécéssite la présentation d'une clé à chaque extrémité de façon à chiffrer et déchiffrer les informations. De plus, comme cet algorithme est symétrique, c'est la même clé qui est utilisée pour chiffrer et déchiffrer.

Un problème important est donc posé par l'acheminement de cette clé afin d'en assurer la sécurité.

Pour sauvegarder cette sécurité, il ne faut pas que la clé soit transmise d'un terminal émetteur vers un terminal récepteur par l'intermédiaire de la ligne de transmission qui relie ces deux terminaux. Dans ces conditions, la clé doit être connue à l'avance des personnes qui désirent

dialoguer entre elles. Lorsque que l'on est en présence d'un organisme émetteur unique, on peut envisager une distribution hiérarchisée de ces clés pour chaque personne utilisatrice, mais cela ne peut pas se généraliser à un réseau complexe notamment public.

- Une deuxième famille de systèmes comprend les systèmes de chiffrement à clé publique et permet de résoudre le problème du transfert des clés en utilisant un algorithme public fondé sur deux fonctions inverses l'une de l'autre. L'une de ces fonctions est publique alors que l'autre fonction est secrète. Un tel algorithme est dissymétrique car les opérations de chiffrement et de déchiffrement correspondent à des fonctions différentes mettant en oeuvre des clés différentes : une fonction publique associée à une clé publique et une fonction inverse associée à une clé secrète. Ces fonctions sont telles qu'en connaissant la fonction publique, il est pratiquement impossible d'en déduire la fonction inverse au sens de la complexité du calcul et du temps nécéssaire à l'obtention du résultat.

La plus connue des fonctions à clé publique est la mise en oeuvre du théorème de d'EULER suivant le schéma préconisé par Rivest, Shamir et Adleman.

Ces fonctions à clé publique sont particulièrement bien adaptées pour résoudre les problèmes d'identification, d'authentification et de protection des transmissions d'informations dès lors que les temps de calcul ne sont pas prohibitifs et que les clés secrètes sont effectivement bien protégées.

Jusqu'à maintenant, la solution consistait à faire exécuter la fonction secrète par un organe isolé et protégé, en général sous la forme d'une "boite noire"

incorporée aux appareils. Cette solution suppose donc que l'appareil détient au moins une clé secrète, ce qui le rend particulièrement vulnérable, surtout s'il doit se trouver dans un lieu public à des fins d'utilisation banalisées mais demandant une certaine sécurité.

L'invention vise à pallier cet inconvénient majeur inhérent à la conception actuelle des systèmes de chiffrement à clé publique formant la deuxième famille précitée. Pour cela, l'invention prévoit de ne plus faire exécuter la fonction secrète dans les appareils qui, dans ces conditions, ne renferment plus aucun secret.

L'invention propose donc un système pour chiffrer et déchiffrer des informations, du type utilisant un système de chiffrement à clé publique constitué d'une part, d'une fonction publique utilisée pour chiffrer une information et/ou vérifier une signature, et d'autre part, de sa fonction inverse secrète utilisée pour déchiffrer un cryptogramme et/ou signer une information ; ledit système comprenant au moins :

- un dispositif électronique disposant d'une première mémoire dans laquelle est enregistré un algorithme correspondant à l'exécution de ladite fonction inverse, d'une seconde mémoire protégée dans laquelle est enregistrée ladite clé secrète, et d'un microprocesseur pour exécuter ledit algorithme ;

- un appareil disposant au moins de circuits de traitement pour fournir audit microprocesseur des informations à traiter et pour exploiter des informations traitées par ledit microprocesseur ;

caractérisé en ce que ledit dispositif électronique se trouve dans un support portatif amovible connectable audit appareil.

Un des avantages importants de l'invention est de permettre la conception et la réalisation d'appareils qui peuvent être mis à la disposition du public sans risquer de tenter un fraudeur de prendre connaissance d'un secret susceptible de remettre en cause le système. Dorénavant, les calculs relatifs à la fonction secrète sont exécutés uniquement dans un support portatif amovible à partir de paramètres enregistrés dans une mémoire protégée de ce support.

L'invention est exposée ci-après plus en détails à l'aide de dessins représentant seulement un mode d'exécution.

La figure 1 représente le principe d'un système conforme à la présente invention.

La figure 2 représente une extension du système représenté à la figure 1.

En se référant à la figure 1, le système conforme à l'invention comprend un dispositif électronique (1) et un appareil (A1) constitués et connectés l'un à l'autre de la façon décrite ci-dessous.

Le dispositif électronique (1) comprend :

- un microprocesseur (2) comprenant lui-même au moins une mémoire (M1), telle qu'une mémoire morte permanente, et des circuits de traitement (T1) ;

- et une mémoire protégée (M2) telle qu'une mémoire morte programmable reliée au microprocesseur (2) par un bus (b1).

Selon l'invention, ce dispositif électronique (1) se trouve dans un support portatif amovible (C1). A titre

d'exemple, ce support (C1) peut être une carte analogue à des cartes de crédit.

L'appareil (A1) comprend au moins une mémoire (MA1) et des circuits de traitement (TA1), et peut être équipé d'un clavier (CA1) et d'un dispositif de visualisation (VS1). Ces différents éléments sont reliés entre eux par un bus (b2).

Le support portatif amovible (C1) dénommé ci-après carte (C1) est connectable à l'appareil (A1) par l'intermédiaire d'une interface (I) telle que celle proposée à l'AFNOR dans le cadre de la normalisation sur les cartes à microcircuits à contacts (Commission CFTC 97/SC 17/GT4). Cette interface (I) peut être schématiquement représentée par un circuit d'interconnexion (IC) prévu au niveau de la carte (C1), d'un dispositif d'interconnexion (IA) prévu au niveau de l'appareil (A1), ces deux dispositifs d'interconnexion étant reliés entre eux par une ligne de transmission (L).

Un système de chiffrement à clé publique se décompose comme suit :

- une fonction publique traduite par un algorithme qui prend en compte une clé publique,

- et une fonction secrète traduite par un algorithme public ou secret qui prend en compte une clé secrète, fonction qui est l'inverse de la fonction publique précitée.

Dans l'exemple représenté à la figure 1, l'algorithme correspondant à la fonction secrète précitée est enregistré dans la mémoire (M1) du microproceseur (2). Cet algorithme n'a pas besoin d'être gardé secret, mais par

contre la clé secrète nécéssaire à l'exécution de cet algorithme doit être gardée secrète. Cette clé est enregistrée dans la mémoire protégée (M2).

L'algorithme correspondant à la fonction à clé publique est par exemple enregistré dans la mémoire (MA1) de l'appareil (A1). Ainsi, toute information, par exemple entrée au clavier (CA1) de l'appareil (A1), peut être chiffrée à l'aide d'une clé publique (P). Pour cela, les circuits de traitement (TA1) de l'appareil (A1) exécutent l'algorithme public en prenant en compte les paramètres suivants : l'information (M) entrée au clavier (CA1) et la clé publique (P) qui est soit également entrée au clavier (CA1), soit préenregistrée dans la mémoire (MA1). L'information ainsi chiffrée est ensuite transmise à la carte (C1) qui va déchiffrer cette information et retrouver l'information initiale (M). Pour cela, le microprocesseur (2) de la carte (C1) exécute l'algorithme correspondant à la fonction à clé secrète (S) associée à la fonction à clé publique utilisée par l'appareil (A1), algorithme qui prend en compte la clé secrète (S) de cette fonction inverse préenregistrée dans la mémoire (M2) du dispositif électronique (1) de la carte (C1). Seule une carte (C1) possédant la clé secrète (S) est capable de déchiffrer l'information chiffrée par l'appareil (A1).

A titre d'exemple, il va être considéré ci-dessous un système de chiffrement à clé publique du type R.S.A.. Cette fonction s'exprime simplement sous la forme :

$C = M^e$ modulo $\underline{n}$

où :

- M est l'information à traiter,
- $\underline{n}$ est le produit d'au moins deux nombres premiers élevés (p) et (q),
- e est un nombre entier premier avec (p-1) et (q-1),
- C est l'information chiffrée ou résultat.

Le nombre (n) est par exemple de la forme
$\underline{n} = 2^{4x} + K$, avec K compris entre 2^{3x} et 2^{3x-1}.

La valeur de (x) est avantageusement quantifiée en classes normalisées, de manière à permettre au concepteur d'un système de faire aisément les compromis nécessaires entre les performances technologiques et la sécurité requise par l'application envisagée. Il est suggéré :
$4x = 2^i \cdot (64 + 16j)$, avec $i, j \in \{(0,1,2,3)\}$

En outre, la concaténation de (i) et (j) en binaire forme un nombre hexadécimal, soit :
$icl = 4i + j$, avec icl de manière à obtenir $icl \in \{0,1,\ldots F\}$
et donne ainsi les correspondances ci-dessous.

Classe icl	0	1	2	3	4	5	6	7	8	9
4x	64	80	96	112	128	160	192	224	256	320

Classe icl	A	B	C	D	E	F
4x	384	448	512	640	768	896

En pratique :
- les classes de 0 à 5 ne présentent pas de sécurité mais elles sont utiles pour la mise au point des programmes et des procédures ;
- les classes de 6 à A sont utilisables avec une sécurité intéressante ;
- les classes de B à F nécessitent une technologie avancée.

Le nombre (e) est par exemple choisi égal à 3 et les deux nombres premiers (p) et (q) sont congrus à 2 modulo 3.

Dans l'exemple de la fonction R.S.A. ainsi donnée, la fonction publique consiste à élever au cube modulo (n) une information à chiffrer, et la fonction secrète consiste à extraire la racine cubique modulo (n) de l'information chiffrée pour retrouver cette information en clair.

Soit (p) un nombre premier impair congru à deux modulo trois (p est de la forme 6k + 5). Quand on calcule modulo (p), extraire la racine cubique est alors équivalent à élever à la puissance (2p-1)/3 soit (=4k+3) ; car 3 et (2p-1)/3 sont alors inverses modulo (p-1).

Ainsi, connaissant la décomposition d'un nombre (n) en facteurs premiers distincts de la forme (6k+5), on peut aisément prendre la racine cubique d'un nombre modulo chacun des facteurs, et ensuite reconstituer le résultat modulo le produit des facteurs.

La clé publique est donc constituée par un nombre composite (n) tandis que la clé secrète est constituée par les facteurs de (n). Pour connaître la clé secrète à partir du nombre (n), il faut donc factoriser ce nombre (n).

La fonction publique est délibérément simplifiée par de telles spécifications ; la description d'un paramètre public se réduit à K soit 3x bits, et l'exécution d'une fonction publique se réduit à deux multiplications modulo (n).

La forme de (n) simplifie considérablement l'opération de réduction modulo (n) en évitant d'effectuer une division.

Soit : $Y = A + 2^{4x} B$ avec $0 \leq A \leq 2^{4x}$

$Y = (A-B.K) + B\ (2^{4x} + K) \equiv (A - B\ K) \bmod n$

si B s'écrit sur moins de x bits, alors B K s'écrit sur moins de 4x bits et il en est en général de même pour A-B K.

Si B s'écrit sur plus de x bits, A-B K s'écrit sur x bits de moins que A.

Les espaces de définition des fonctions des différents usagers ne coïncident pas, car les nombres (n) sont différents. Quand il faut constituer un résultat en appliquant successivement des fonctions publiques ou secrètes de plusieurs usagers, il se peut qu'un résultat intermédiaire soit supérieur au nombre composite de la fonction suivante, et ceci est une source de difficulté dans la conception et la mise en oeuvre des procédures.

Quand toutes les fonctions considérées appartiennent à une même classe, les spécifications choisies ici rendent si faible la probabilité de rencontrer accidentellement de tels incidents qu'il n'y a pas lieu d'en tenir compte dans la programmation des applications.

L'éxécution d'une telle fonction R.S.A. nécéssite donc des circuits de multiplication. En pratique, soit les circuits de traitement (T1) du microprocesseur (2) incluent de tels circuits de multiplication, soit ces circuits de multiplication sont ajoutés et reliés aux circuits de traitement (T1). Dans ce dernier cas, les circuits de multiplication MUL sont réalisés, d'une façon connue en soi, soit par des circuits câblés, soit par des circuits microprogrammés.

En se référant à la figure 2, il est illustré une extension du sytème conforme à l'invention. Cette

extension consiste à relier l'appareil (A1) à un appareil (A2) par l'intermédiaire d'une interface (I1) constituée d'un circuit d'interconnexion (IA1) au niveau de l'appareil (A1), d'un circuit d'interconnexion (IA2) au niveau de l'appareil (A2) et d'une ligne de transmission (L1) entre ces deux circuits (IA1), (IA2). Cet appareil (A2) est par exemple identique à l'appareil (A1) (mémoire MA2, circuits de traitement TA2, clavier CA2 et dispositif de visualisation VS2).

Une carte (C2) du même type que la carte (C1) peut être connectable à l'appareil (A2) par l'interface (I) précité.

Il va être décrit ci-après deux exemples d'application d'un système conforme à l'invention en référence aux figures 1 et 2.

Soit une personne (X1) qui désire envoyer un message confidentiel (M) à une personne (X2). La personne (X1) est personnalisée par une clé publique (P1) et par une clé secrète (C1). Cette personne (X1) est titulaire d'une carte (C1) dont la mémoire protégée (M2) renferme la clé secrète (S1) et dont la mémoire (M1) contient un algorithme correspondant à la fonction secrète inverse d'une fonction publique du type R.S.A. précitée. La personne (X2) est personnalisée par une clé publique (P2) et par une clé secrète (S2), et est titulaire d'une carte (C2).

La personne (X1) entre son message (M) au clavier (CA1) de l'appareil (A1). Ce message (M) est chiffré par les circuits de traitement (TA1) de l'appareil (A1). Ces circuits (TA1) exécutent l'algorithme public de la fonction R.S.A. préenregistré dans la mémoire (MA1) de l'appareil (A1). La clé de chiffrement utilisée est la clé publique (P2) de la personne (X2). Cette clé (P2) est par

exemple répertoriée dans un annuaire. Le message chiffré est ensuite transmis par la ligne de transmission (L1) à l'appareil (A2).

La personne (X2) connecte sa carte à l'appareil (A2). Le message chiffré reçu par l'appareil (A2) est transmis aux circuits de traitement (TA2) de la carte (C2). Ces circuits de traitement (TA2) exécutent l'algorithme de la fonction secrète préenregistré dans la mémoire (M1) de la carte (C2). Cet algorithme prend en compte la clé secrète (S2) préenregistrée dans la mémoire (M2). L'exécution de la fonction secrète permet de restituer en clair le message (M). Ce message (M) est par exemple affiché sur le disposifif de visualisation (VS2). Ainsi, seule la personne (X2), personnalisée par la clé secrète (S2), est susceptible de déchiffrer le message.

Dans une telle application, la personne (X2) ne peut pas certifier que le message a été effectivement transmis par la personne (X1). Autrement dit, la personne (X2) ne peut pas authentifier la signature du message transmis.

Cependant, la fonction R.S.A. présente la particularité qu'un message traité par la fonction secrète peut être restitué par la fonction publique. Dans ces conditions, la personne (X1) peut très bien produire une signature avec sa clé secrète, signature qui sera vérifiée par la personne (X2) en utilisant la clé publique (P1) de la personne (X1). Ainsi, la personne (X2) pourra certifier cette signature, étant donné que seule la personne (X1) est à même d'élaborer une telle signature.

Le système conforme à l'invention peut être également utilisé pour transmettre des clés de chiffrement et de déchiffrement. En effet, il est parfaitement possible d'utiliser des algorithmes de chiffrement plus simples et

plus rapides tels que ceux de la première famille précitée, et de les combiner avec un algorithme à clé publique. En d'autre termes, un message (M) à transmettre est chiffré par un algorithme de chiffrement conventionnel utilisant une clé secrète (S). Le problème réside alors dans la transmission de cette clé secrète (S). Pour cela, il suffit de chiffrer cette clé secrète par une fonction publique du type R.S.A.. La clé de chiffrement utilisée est la clé publique de la personne à laquelle est destiné le message chiffré. Il suffit ensuite que la personne à laquelle est destiné ce message applique sa fonction secrète sur cette clé chiffrée pour retrouver la clé de déchiffrement du message.

A titre d'exemple, il est possible d'utiliser des microprocesseurs du type "INTEL 8751" pour exécuter la fonction R.S.A. précitée.

Bien évidemment, ces deux applications n'ont été données qu'à titre d'illustration. Il est en effet possible d'appliquer le principe de l'invention à bon nombre d'applications en faisant éventuellement intervenir d'autres paramètres spécifiques des applications envisagées.

REVENDICATIONS

1. Système pour chiffrer et déchiffrer des informations, du type utilisant un système de chiffrement à clé publique constitué d'une part, d'une fonction publique utilisée pour chiffrer une information et/ou vérifier une signature, et d'autre part, de sa fonction inverse secrète utilisée signer une information et/ou déchiffrer un cryptogramme ; ledit système comprenant au moins :

- un dispositif électronique (1) disposant au moins d'une première mémoire (M1) dans laquelle est enregistré un algorithme correspondant à l'exécution de ladite fonction inverse, d'une seconde mémoire protégée (M2) dans laquelle sont enregistrés les paramètres secrets (S) de la fonction inverse, et d'un microprocesseur (2) pour exécuter ledit algorithme ;

- un appareil (A1) disposant au moins de circuits de traitement (TA1) pour fournir audit microprocesseur (2) des informations à traiter et pour exploiter des informations traitées par ledit microprocesseur (2) ;

caractérisé en ce que ledit dispositif électronique (1) se trouve dans un support portatif amovible (C1) connectable audit appareil (A1).

2. Système selon la revendication 1, caractérisé en ce que la première mémoire (M1) précitée contient également un algorithme correspondant à l'exécution de la fonction publique précitée.

3. Système selon la revendication 1, caractérisé en ce que l'appareil (A1) précité comprend une mémoire (MA1) dans laquelle est enregistré un algorithme correspondant à l'exécution de la fonction publique précitée.

4. Système selon l'une des revendications précédentes, caractérisé en ce qu'il comprend en plus au moins un

second appareil (A2) disposant au moins d'une mémoire (MA2) dans laquelle est enregistré un algorithme correspondant à l'exécution de la fonction publique précitée, de circuits de traitement (TA2) pour fournir au premier appareil précité A1) des informations traitées par ledit algorithme et/ou pour recevoir des informations traitées par ledit premier appareil (A1), lesdits appareils étant reliés entre eux par une ligne de transmission (L1).

5. Système selon la revendication 4, caractérisé en ce que le second appareil (A2) précité est connecté à un second support électronique portatif amovible (C2) disposant au moins d'une première mémoire (M1) dans laquelle est enregistré l'algorithme précité correspondant à l'exécution de la fonction inverse précitée, d'une seconde mémoire (M2) protégée dans laquelle sont enregistrés les paramètres secrets (S1) de la fonction inverse, et d'un microprocesseur (2) pour exécuter ledit algorithme ; et en ce que lesdits paramètres secrets (S1) enregistrés dans le support (C2) sont différents de ceux (S) enregistrés dans le premier support (C1).

6. Système selon l'une des revendications précédentes, dans lequel la fonction à clé publique précitée connue sous le nom de RSA est de la forme $C = M^e$ modulo $\underline{n}$ où :

- M est un nombre entier de 0 à n-1 représentant l'information à traiter,
- $\underline{n}$ est le produit d'au moins deux nombres premiers élevés (p) et (q),
- $\underline{e}$ est un nombre entier premier avec (p-1), (q-1),
- C est un nombre entier de 0 à n-1 représentant l'information traitée ou résultat,

caractérisé en ce que le nombre $\underline{n}$ est de la forme $n = 2^{4x} + K$, avec K compris entre 2^{3x} et 2^{3x-1}

x étant un nombre entier égal à

$2^i \cdot (64 + 16j)$ $i, j, \in \{0, 1, 2, 3\}$

7. Système selon la revendication 6, caractérisé en ce que le nombre e est égal à 3, les nombres premiers facteurs de (n) étant de la forme 6k+5.

8. Système selon l'une des revendications précédentes, caractérisé en ce que chaque support électronique portatif amovible (C1, C2) précité comprend des circuits (MUL) pour effectuer des multiplications de nombres.

9. Système selon la revendication 8, caractérisé en ce que les circuits multiplicateurs (MUL) précités sont réalisés par des circuits câblés.

10. Système selon la revendication 8, caractérisé en ce que les circuits multiplicateurs (MUL) précités sont réalisés par des circuits microprogrammés.

11. Système selon la revendication 8, caractérisé en ce que les circuits multiplicateurs (MUL) précités sont intégrés dans le microprocesseur (2).

12. Système selon la revendication 1 ou 5, caractérisé en ce que chaque première mémoire (M1) précitée est la mémoire du microprocesseur (2).

13. Système selon la revendication I2, caractérisé en ce que chaque seconde mémoire (M2) précitée est une mémoire morte programmable.

14. Support électronique portatif amovible pour chiffrer et déchiffrer des informations, du type utilisant un système de chiffrement à clé publique constitué d'une part, d'une fonction publique utilisée pour chiffrer une information et/ou vérifier une signature et d'autre part, de sa fonction inverse secrète utilisée pour signer une information et/ou déchiffrer un cryptogramme ; caractérisé en ce que ledit support (C1) comprend au moins une première mémoire (M1) où est enregistré un algorithme

correspondant à l'exécution de la fonction inverse secrète (S) précitée, une seconde mémoire protégée (M2) où sont enregistrés lesdits paramètres secrets (S) et un microprocesseur (2) pour exécuter ledit algorithme.

15. Support selon la revendication 14, caractérisé en ce que la mémoire précitée (M1) dudit support (C1) contient également un algorithme correspondant à l'exécution de la fonction publique précitée.

16. Support selon la revendication 14, caractérisé en ce que le support électronique portatif amovible (C1) comprend des circuits (MUL) pour effectuer des multiplications de nombres.

17. Support selon la revendication 16, caractérisé en ce que les circuits multiplicateurs (MUL) précités sont réalisés par des circuits câblés.

18. Support selon la revendication 16, caractérisé en ce que les circuits multiplicateurs (MUL) précités sont réalisés par des circuits microprogrammés.

19. Support selon la revendication 16, caractérisé en ce que les circuits multiplicateurs (MUL) précités sont intégrés dans le microprocesseur (2) dudit support (C1).

20. Support selon l'une des revendications 14 à 19, caractérisé en ce qu'il est constitué par une carte (C1).

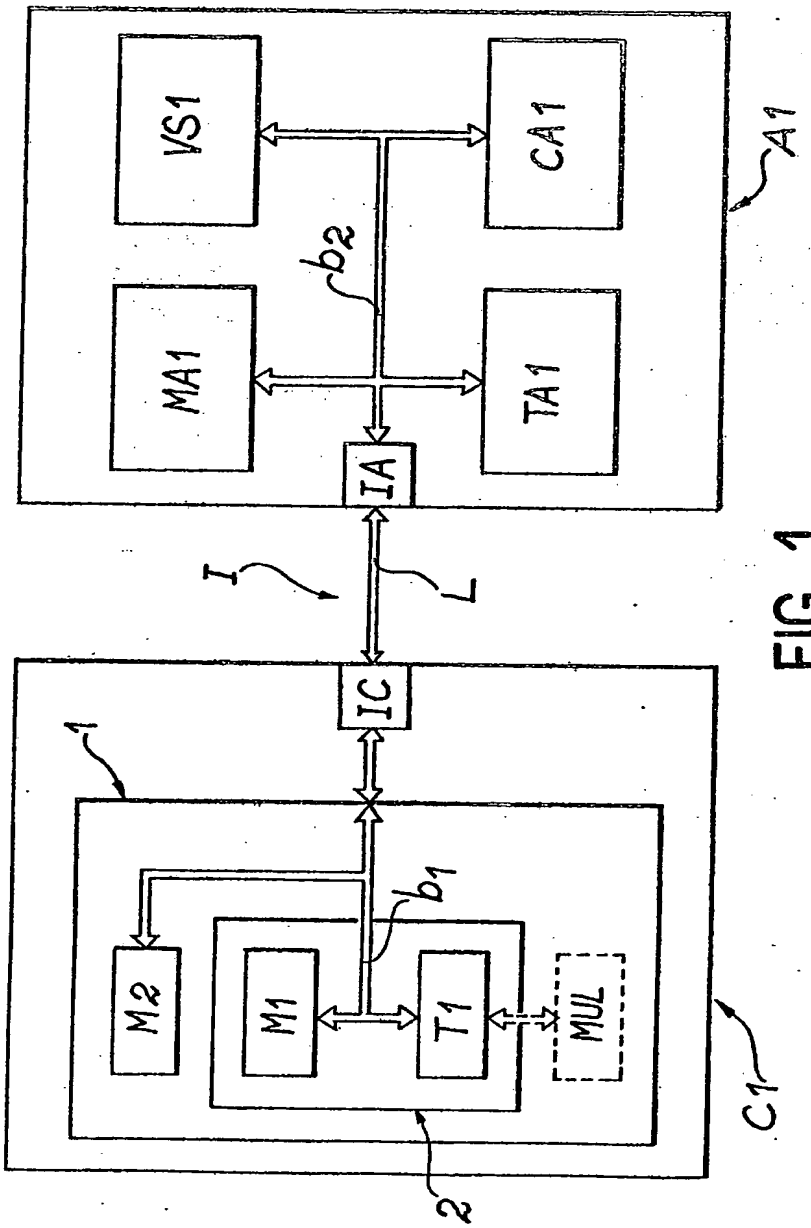


FIG. 1

2536928

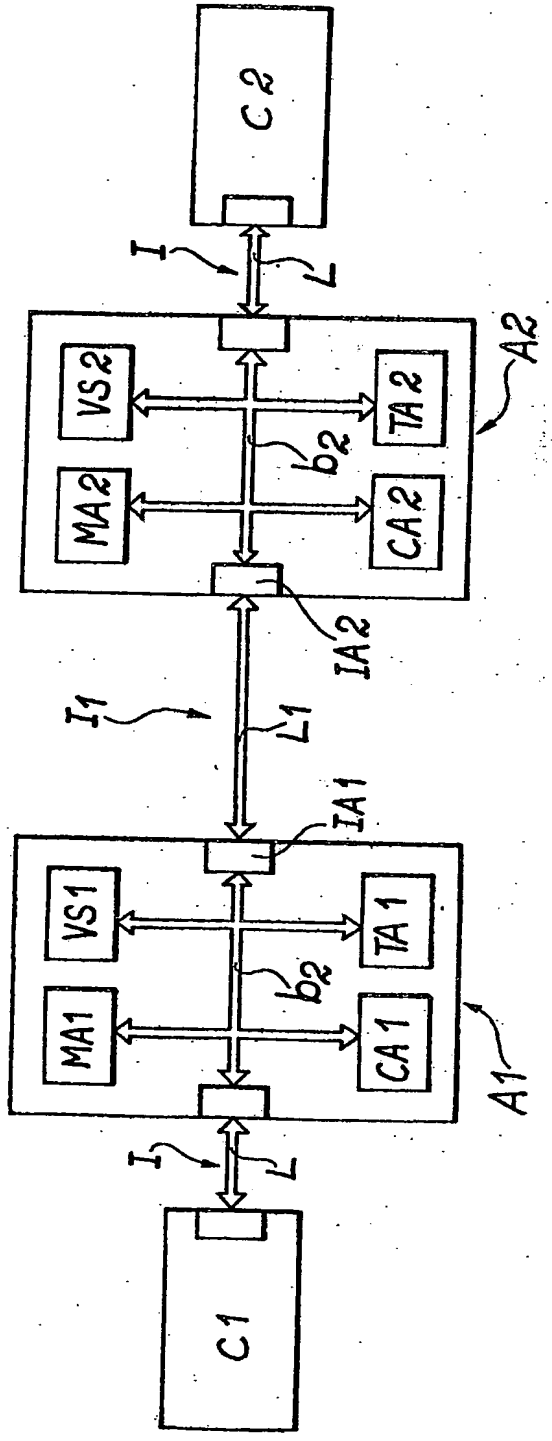


FIG. 2